UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/554,419	05/11/2000	LYNN SPRAGGS	PA1065US	6883

7590 07/03/2002

AARON WININGER
CARR & FERRELL
2225 EAST BAYSHORE ROAD
SUITE 200
PALO ALTO, CA 94303

EXAMINER	
SMITHERS, MATTHEWS	

ART UNIT	PAPER NUMBER
2132	8

DATE MAILED: 07/03/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/554,419	SPRAGGS, LYNN	
	Examiner	Art Unit	
	Matthew B Smithers	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 April 2002* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *15-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *15-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Status of Application

Claims 1-14 were canceled.

Claims 15-47 were added.

Claims 15-47 are pending.

Response to Arguments

Applicant's arguments with respect to claims 15-47 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

Claims 44-47 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claims 44, 45, 46 and 47 are method claims that depend from a computer-readable medium claim 42.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 15-30 and 38-47 are rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Specifically, support for "encrypt data independently of an identity of the client" could not be found in the specification.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in-
> (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effect under this subsection of a national application published under section 122(b) only if the international application designating the United States was published under Article 21(2)(a) of such treaty in the English language; or
> (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that a patent shall not be deemed filed in the United States for the purposes of this subsection based on the filing of an international application filed under the treaty defined in section 351(a).

Claims 15-47 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. patent 6,065,120 granted to Laursen et al.

Regarding claim 15, Laursen meets the claimed limitations as follows:

"A system for using a shared key to transmit secure data between a client and a server, the system comprising:

an encrypt/ decrypt engine for using the shared key to encrypt or decrypt data, the encrypt/ decrypt engine being configured for delivery via a web page to

a client in response to a user request and further configured to encrypt data independently of an identity of the client;

wherein the server includes a user private keys database configured to store the shared key." see column 9, line 33 to column 15, line 25.

Regarding claim 16, Laursen meets the claimed limitations as follows: **"The system of claim 15 wherein the shared key is a user's private key entered by a user into the web page."** see column 9, lines 17-25; column 9, lines 33- 54; column 13, line 41 to column 14, line 6 and column 14, line 40 to column 15, line 13.

Regarding claim 17, Laursen meets the claimed limitations as follows: **"The system of claim 15 further comprising a secure data database configured to store data received from the client and, upon the completion of a processing step, to deliver the stored data in an encrypted format to the client or to another client."** see column 15, lines 14-21.

Regarding claim 18, Laursen meets the claimed limitations as follows: **"The system of claim 15 further comprising a secure data database configured to store data received from the client and, upon receipt of a request for the data, to deliver the stored data in an encrypted format to the client or to another client."** see column 15, lines 14-21.

Regarding claim 19, Laursen meets the claimed limitations as follows: **"The system of claim 15 wherein the shared key is transmitted between the server and the client as few as zero times and the shared key is transmitted between the server and the user as few as one time."** see column 9, line 33 to column 13, line 9.

Regarding claim 20, Laursen meets the claimed limitations as follows: **"The system of claim 15 wherein the shared key is a user's private key entered by a user."** see column 9, lines 17-25; column 9, lines 33- 54; column 13, line 41 to column 14, line 6 and column 14, line 40 to column 15, line 13.

Regarding claim 21, Laursen meets the claimed limitations as follows: **"The system of claim 15 wherein the client encrypt/ decrypt engine is installed on the client. "** see column 9, line 59 to column 10, line 62.

Regarding claim 22, Laursen meets the claimed limitations as follows: **"A system for using a shared key in transmitting secure data between a client and a server, the system comprising:**

an encrypt/decrypt engine for using the shared key in encrypting data, the encrypt/decrypt engine being configured to encrypt data independently of an identity of the client;

and a user private keys database located on the server and configured to store the shared key, the shared key being the private key of a user." see column 9, line 33 to column 15, line 25.

Regarding claim 23, Laursen meets the claimed limitations as follows: **"The system of claim 22 wherein the server is configured to decrypt encrypted data received from the client using the shared key and to use a private server key to re-encrypt the decrypted data."** see column 12, line 60 to column 13, line 9.

Regarding claim 24, Laursen meets the claimed limitations as follows:

"The system of claim 23 further comprising a secure data database configured to store the encrypted data received from the client and re-encrypted by the server and to deliver the stored data to the client or to another client; the delivered data, after the completion of a processing step, being encrypted with the shared key or with another shared key. " see column 15, lines 14-21.

Regarding claim 25, Laursen meets the claimed limitations as follows:

"The system of claim 23 further comprising a secure data database configured to store the encrypted data received from the client and re-encrypted by the server and to deliver the stored data to the client or to another client; the delivered data being, upon receipt of a request for the data, encrypted with the shared key or with another shared key. " see column 15, lines 14-21.

Regarding claim 26, Laursen meets the claimed limitations as follows:

"The system of claim 25 wherein the request is from the user." see column 13, line 41 to column 14, line 28.

Regarding claim 27, Laursen meets the claimed limitations as follows:

"The system of claim 25 wherein the request is from an other user." see column 15, lines 14-21.

Regarding claim 28, Laursen meets the claimed limitations as follows:

"A system for using a shared key in transmitting secure data between a client and a server, the system comprising:

an encrypt/decrypt engine for using the shared key entered by a user to encrypt data entered by the user, the encrypt/decrypt engine being configured

such that all data entered by the user and stored on the client is stored in encrypted form, and further configured to encrypt data independently of an identity of the client;

the server including a user private keys database configured to store the shared key, the shared key being a private key of a user; and the client." see column 9, line 33 to column 15, line 25.

Regarding claim 29, Laursen meets the claimed limitations as follows: **"The system of claim 28, wherein the encrypt/decrypt engine uses a symmetric key encryption/ decryption algorithm for encrypting and decrypting data."** see column 10, lines 42-62.

Regarding claim 30, Laursen meets the claimed limitations as follows: **"The system of claim 28, further including a web server engine configured for the user to securely send or receive data from the client to the server."** see column 11, line 43 to column 12, line 44.

Regarding claim 31, Laursen meets the claimed limitations as follows: **"A method for using a shared key in receiving secure data on a server, comprising the steps of:**

delivering from a server to a client a web page including an encrypt/ decrypt engine;

encrypting data on the client using the encrypt/decrypt engine and a shared key entered by a user of the client, the shared key being shared between the user and the server;

delivering the encrypted data from the client to the server;

receiving the encrypted data at the server, decrypting the encrypted data at the server using the shared key;

and processing the decrypted data." see column 9, line 33 to column 15, line 25.

Regarding claim 32, Laursen meets the claimed limitations as follows:

"The method of claim 31, wherein the step of processing the decrypted data includes the steps of:

encrypting the decrypted data with a private server key; and

storing the encrypted data in a database." see column 11, line 43 to column 12, line 44.

Regarding claim 33, Laursen meets the claimed limitations as follows:

"The method of claim 31, wherein the step of processing the decrypted data includes the steps of:

re-encrypting the data with an other user's private key shared between the other user and the server; and sending the re-encrypted data to the other user." see column 9, line 33 to column 15, line 25.

Regarding claim 34, Laursen meets the claimed limitations as follows:

"The method of claim 31, wherein the step of processing the decrypted data includes the steps of:

decrypting the encrypted data with the private server key;

re-encrypting the data with a second user's key shared between the second user and the server; and sending the re-encrypted data to the second user." see column 13, line 41 to column 14, line 28 and column 15, lines 14-25.

Regarding claim 35, Laursen meets the claimed limitations as follows:

"The method of claim 31, wherein the step of processing the decrypted data includes the steps of:

processing the data according to an instruction of the user;

re-encrypting the processed data using the user's shared key;

and sending the re-encrypted processed data to the user. " see column 13, line 41 to column 14, line 28 and column 15, lines 14-25.

Regarding claim 36, Laursen meets the claimed limitations as follows:

"The method of claim 31, wherein the step of processing the decrypted data includes storing the decrypted data in a secure database." see column 2, line 58 to column 3, line 17; column 9, line 33 to column 15, line 25.

Regarding claim 37, Laursen meets the claimed limitations as follows:

"A computer-readable medium comprising program instructions for causing a computer system to use a shared key in receiving secure data at a server, by the steps of:

delivering a web page from the server to a client, the web page including an encrypt/decrypt engine and being configured to use the encrypt/decrypt engine and a shared key entered by a user of the client to encrypt data on the client, the shared key being shared between the user and the server;

receiving the encrypted data at the server;

decrypting the encrypted data using the shared key; and processing the decrypted data." see column 9, line 33 to column 15, line 25.

Regarding claim 38, Laursen meets the claimed limitations as follows:

"A computer-readable medium comprising program instructions for causing a computer system to receive secure data on a server using a shared key, by the steps of:

delivering a encrypt/decrypt engine from the server to a client, the encrypt/decrypt engine being configured to use a shared key entered by a user of the client to encrypt data on the client, the shared key being shared between the user and the server and the encryption being independent of an identity of the client;

receiving the encrypted data at the server;

decrypting the encrypted data using the shared key; and processing the decrypted data." see column 9, line 33 to column 15, line 25.

Regarding claim 39, Laursen meets the claimed limitations as follows:

"The computer readable medium of claim 38, further comprising program instructions for causing the processed decrypted data to be re-encrypted using a private server key." see column 11, line 43 to column 12, line 44.

Regarding claim 40, Laursen meets the claimed limitations as follows:

"The computer-readable medium of claim 39, further comprising program instructions for causing the processed decrypted data to be stored in a secure

database." see column 2, line 58 to column 3, line 17; column 9, line 33 to column 15, line 25.

Regarding claim 41, Laursen meets the claimed limitations as follows: **"The computer-readable medium of claim 38, wherein processing the decrypted data includes the steps of:**

re-encrypting the data with the private server key;

storing the re-encrypted data;

decrypting the stored data with the private server key;

encrypting the data with a second user's key shared between the second user and the server; and sending the encrypted data to the second user." see column 9, line 33 to column 15, line 25.

Regarding claim 42, Laursen meets the claimed limitations as follows: **"The computer-readable medium of claim 38, wherein processing the decrypted data includes the steps of:**

processing the data according to an instruction of the user;

encrypting the processed data using a shared key; and

sending the encrypted processed data to the user or to another user." see column 9, line 33 to column 15, line 25.

Regarding claim 43, Laursen meets the claimed limitations as follows: **"A method of using a shared key in transmitting secure data between a client and a server using a shared key, comprising the steps of:**

encrypting data using the shared key with an encrypt/ decrypt engine configured to encrypt data independently of an identity of the client, the shared key being entered by a user of the client;

delivering the encrypted data from the client to the server;

receiving the encrypted data at the server;

decrypting the encrypted data at the server using the shared key, the shared key being stored in a user private keys database; and processing the decrypted data." see column 9, line 33 to column 15, line 25.

Regarding claim 44, Laursen meets the claimed limitations as follows:

"The method of claim 42, wherein processing the decrypted data includes the steps of:

encrypting the decrypted data with a private server key; and storing the encrypted data in a database." see column 9, line 33 to column 15, line 25.

Regarding claim 45, Laursen meets the claimed limitations as follows:

"The method of claim 42, wherein the step of processing the decrypted data includes the steps of:

encrypting the data with an other user's private key shared between the other user and the server; and sending the encrypted data to the other user." see column 9, line 33 to column 15, line 25.

Regarding claim 46, Laursen meets the claimed limitations as follows:

"The method of claim 42, wherein the step of processing the decrypted data includes the steps of:

decrypting the re-encrypted data with the private server key;

encrypting the data with a second user's key shared between

the second user and the server; and sending the encrypted data to the second user." see column 9, line 33 to column 15, line 25.

Regarding claim 47, Laursen meets the claimed limitations as follows:

"The method of claim 42, wherein the step of processing the decrypted data includes the steps of:

processing the data according to an instruction of the user;

re-encrypting the processed data using the user's shared key;

and sending the re-encrypted processed data to the user." see column 9, line 33 to column 15, line 25.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Bodnar (6,061,790) discloses a mutual authentication procedure between a client and a server where the communication between the two is initiated by the client's password.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (703) 308-9293. The examiner can normally be reached on Monday-Friday (9:00-5:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Matthew Smithers
June 29, 2002

Matthew B Smithers